IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	1:14-CR-322 (JCC)
	)	
RALPH FREEMAN,	)	
	)	
Defendant.	)	

M E M O R A N D U M O P I N I O N

On September 25, 2014, a federal grand jury returned a two-count indictment charging Defendant Ralph Freeman ("Defendant") with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) ("Count One") and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4) ("Count Two"). [Dkt. 16.] On November 20, 2014 [Dkt. 49], and again on the first day of trial on November 24, 2014, Defendant waived his Sixth Amendment right to a trial by jury and requested a bench trial by this Court. The bench trial concluded on November 25, 2014. The parties submitted proposed findings of fact and conclusions of law on December 18, 2014 [Dkts. 62, 63].

The matter now before the Court is whether Defendant violated 18 U.S.C. § 2252(a)(2) by receiving child pornography, and whether Defendant violated 18 U.S.C. § 2252(a)(4) by

possessing child pornography. For the following reasons, the Court finds Defendant guilty of both Count One and Count Two.

I. Findings of Fact

The evidence presented at trial established the following findings of fact:

A. On April 25, 2013, Department of Homeland Security, Homeland Security Investigations ("HSI") Special Agent Tarrah Romanoff identified an Internet Protocol Address ("Subject IP Address")[1] that used the eDonkey[2] peer-to-peer file sharing network between March 21, 2013 and March 29, 2013. (Trial Tr. [Dkts. 60, 61] at 37.)

B. The Subject IP Address was associated with over one hundred known child pornography files. (Id. at 37-38.)

C. HSI Agent Romanoff viewed two video files associated with the Subject IP Address. Both video files depicted minor females engaged in sexual activity with adult males. (Id. at 38-39.)

D. HSI Agent Romanoff issued a summons to the Internet Service Provider ("ISP") to learn the postal street

[1] An IP Address identifies a particular computer on an internet network. This address is assigned by the internet service provider and is akin to a postal address assigned to street locations by the United States Postal Service. (Trial Tr. at 37).

[2] eDonkey is an open peer-to-peer file sharing network comprised of users on the Internet. (Id. at 37, 57.) eMule is particular software used by users on the eDonkey network to share files with other users. (Id. at 37.) To locate other files in eMule, a user connects to the eMule software using an Internet connection, and then locates files through other users using specific search terms that typically describe the type of file to be downloaded. (Id. at 113.)

address associated with the Subject IP Address. (Id. at 39.)

E. The postal street address associated with the Subject IP Address is 1009 Madison Lane, Falls Church, Virginia 22046 ("the residence"), which is located within the Eastern District of Virginia. (Id.)

F. On July 30, 2013, HSI Agent Romanoff and other state and federal law enforcement officials executed a search warrant at the residence, where Defendant resided, and continues to reside, with his wife, mother-in-law, and some, but not all, of his eight children. (Id. at 39-40.)

G. During the search, law enforcement agents seized the following computer media from the residence, which were all manufactured outside the Commonwealth of Virginia, traveled in interstate commerce, and maintained through a proper chain of custody[3] from the time of seizure to the time they were introduced and admitted into evidence at trial (id. at 46-48):

1. Sony Desktop Computer with Seagate 1.5 TeraByte Hard Drive, SN 9VS111XH (Gov't Exs. 1, 15) ("Sony all-in-one desktop");
2. Apricorn EZ-UPS External USB 500G Hard Drive, SN 5YX135RR (Gov't Ex. 2) ("Apricorn hard drive");

[3] Stipulation No. 2 [Dkt. 57] at 1-2.

3. Sony Vaio Laptop with Crucial 256GB Solid State Drive, SN 11070303510D (Gov't Ex. 3) ("Sony laptop");
4. HP Pavilion Desktop with Western Digital 640GB Hard Drive, SN WCASY0898534 (Gov't Ex. 4);
5. Seagate 1 TeraByte Hard Drive, SN 9VP18MLF (Gov't Ex. 5);
6. Samsung 500GB Hard Drive, SN S10NJ1DPB04210 (Gov't Ex. 6) ("Samsung hard drive");
7. Seagate 500GB Hard Drive, SN 5VE09RM2 (Gov't Ex. 7); and
8. Toshiba 40GB Hard Drive, SN Z4NM31672T (Gov't Ex. 8) ("Toshiba hard drive").

H. Defendant is part owner of two small businesses: Metal Fabulous, a metal fabrication company located in Hyattsville, Maryland, and Abco, a restaurant and foodservice equipment supplier located in Alexandria, Virginia. (Trial Tr. at 61-62, 148.)

I. Defendant regularly creates computer-aided design ("CAD") drawings as part of his work. (Id. at 61-62, 253.)

J. From December of 2011 to July 2014, Brad Martensen ("Brad") worked for Defendant at "Metal Fabulous" as a project manager and shop foreman. (Id. at 61.)

K. Brad regularly used the Sony all-in-one desktop

from January of 2012 until January of 2013 for CAD drawings, excel worksheets, email, and work-related photography, until his job duties changed and he used a different computer. (Id. at 62-65.)

L. At some point after Brad stopped using the Sony all-in-one desktop, it was no longer physically located in the office of Metal Fabulous. (Id. at 64.)

M. The Sony all-in-one desktop was located in the third-floor living room/office space near Defendant's bedroom when law enforcement agents seized it on July 30, 2013. (Id. at 42-45, 78-79; Gov't Ex. 15.)

N. The Sony all-in-one desktop had two user accounts: "Brad" and "Media User." (Trial Tr. at 88-89; Gov't Ex. 39.)

O. The "Brad" account on the Sony all-in-one desktop was not password protected. (Trial Tr. at 89.)

P. Brad never downloaded child pornography files onto the Sony all-in-one desktop, and no child pornography files were located in the "Brad" account on the Sony all-in-one desktop. (Id. at 66, 89; see also Gov't Exs. 40-43.)

Q. The "Media User" account was password protected and the password was "1009," the street number of Defendant's residence. (Trial Tr. at 90; Gov't Ex. 44.)

R. The desktop of the "Media User" account on the Sony all-in-one desktop had shortcut icons for, inter alia, programs related to architectural drawing programs, CAD applications, the eMule software application, and the DropBox cloud storage application registered to the email address "Ralph@metalfabulous.com." (Trial Tr. at 90-92; Gov't Ex. 45.)

S. Defendant used the Sony all-in-one desktop under the "Media User" to conduct work business, personal business, and to download and view child pornography.

T. The "Media User" account on the Sony all-in-one desktop contained six-hundred fifty-four (654) still-image files (Gov't Ex. 21) and forty-nine (49) video files (Gov't Ex. 20) with "hash values"[4] that matched known child pornography file hash values, or child pornography files found in other law enforcement investigations.[5] (Gov't Ex. 23 at 2.)

U. The "Media User" account on the Sony all-in-one desktop contained two-thousand-nine-hundred (2,900) still-image files and one-hundred-eighty (180) video files of suspected child pornography. (Gov't Ex. 23 at 2.)

V. All of the child pornography files found on the

[4] Each file has a unique "digital fingerprint" known as a "hash value." If the file is changed or altered, then the "hash value" also changes. Law enforcement maintains a database of "hash values" that are "digital fingerprints" for known child pornography files. (Trial Tr. at 38-39, 56-57.)

[5] The still-image files and video files in Government Exhibits 20 and 21 depict actual minor children under 18 years of age engaged in sexually explicit conduct that occurred outside the Commonwealth of Virginia. (See Stipulation No. 1 [Dkt. 56].)

Sony all-in-one desktop were located under the "Media User" account. (Trial Tr. at 92.)

W. The "most frequently accessed" file list on the "Media User" account of the Sony all-in-one desktop included, inter alia, child pornography video files with titles that included popular key words associated with child pornography investigations: "pthc" (abbreviation for pre-teen hardcore); "Lilu Planet," and "Peter Boyle" (titles of child pornography known to law enforcement). (Id. at 94-95; Gov't Ex. 46.)

X. The "most frequently accessed" file list in the "7-Zip"[6] file-manager program on the "Media User" account of the Sony all-in-one desktop included files with titles that contained key words associated with other child pornography investigations, including: "Ruby," "HMM Gracel," and "pthc." (Trial Tr. at 94-96; Gov't Ex. 54.)

Y. In the "Media User" account on the Sony all-in-one desktop, all child pornography still-image files were located in the folder "\Users\Media User\Downloads\eMule\Incoming" ("the eMule incoming folder") except one file found within a "Temp" folder. The eMule incoming folder was the default folder where downloaded files

[6] A zip file is an archive file that allows a user to take many files and condense them into one package, which makes it easier to download the files or otherwise store them. (Trial Tr. at 95.)

from eMule were saved or stored. (Trial Tr. at 113-114; Gov't Ex. 23 at 2, Ex. 58.)

Z. In the "Media User" account on the Sony all-in-one desktop, all child pornography video files were located in the eMule incoming folder. (Id.)

AA. Under the "Media User" account on the Sony all-in-one desktop, the eMule incoming folder contained three "subfolders" titled: "Gracel," "HMM Gracel series (Cambodia) - Gracel, Rona, Le…," and "New Folder." "Gracel" and "HMM Gracel series (Cambodia)" are titles of child pornography series previously known to law enforcement through other investigations. (Trial Tr. at 114; Gov't Ex. 58.)

BB. Additional subfolders containing child pornography were found within the "HMM Gracel series (Cambodia)" folder under the "Media User" account on the Sony all-in-one desktop. (Trial Tr. at 114; Gov't Ex. 59.)

CC. The subfolder titled "New Folder" contained thumbnail icons of child pornography video files under the "Media User" account on the Sony all-in-one desktop, including the following file titles:

1. "ok-PTHC 2010 New Pedo 10Yo Little Girl Agnieszka from…"
2. "-Pthc - Real 1 12 Yo muito linda.mpg"

3. "(Children-sf-1man) Gracel Series-Rona (08Yo)-(KINDER).AVI" (Trial Tr. at 114-115; Gov't Ex. 60.)

DD. At the time of the forensic examination of the Sony all-in-one desktop, within the eMule application under the "Media User" account, various child pornography files were "pending" and in various stages of inactive or active download from other eMule users through the Internet.[7] (Trial Tr. at 115-120; Gov't Exs. 61-63.)

EE. March 27, 2013 was the last search date in the eMule application under the "Media User" account on the Sony all-in-one desktop. (Trial Tr. at 117-118.)

FF. Defendant used the following search terms in the eMule application under the "Media User" account on the Sony all-in-one desktop to search for child pornography files to download from other eMule users through the Internet: "agnieszha," "agnieska," agnieszka pthc," barbara pedo," "barbara pthc," "gracel," "greatis," "kassette," "liluplanet," "linda pthc," "pedo," "pedo cam," "pedo webcam," "peter boil," "pthc incest," "pthc incest cam," "pthc poland," "pthc polish,"

[7] HSI Special Agent Jay Varda, who qualified at trial as an expert in computer forensics, testified about the process of downloading files within eMule. Several factors affect how long it takes to download a file, including the size of the file, the Internet download speed, and the number of users downloading the file. (Trial Tr. at 115-116.)

"pthc russia," "pthc webcam," "TMS Component," "TMS Scripter,"[8] "TMS Scripter 6," "TMSScripter," "TMSstudio," "underage," "underage cam," "underage webcam," and "XE3." All of these search terms are key words associated with child pornography. (Trial Tr. at 120-123; Gov't Ex. 64-69.)

GG. Defendant used these search terms in the eMule application under the "Media User" account on the Sony all-in-one desktop after February 2, 2013. (Trial Tr. at 123-125; Gov't Ex. 71.)

HH. Defendant downloaded the four child pornography video files (Gov't Ex. 20) located under the "Media User" account on the Sony all-in-one desktop after using some of the search terms listed above to locate the files on the eMule network. (Trial Tr. 125-130; Gov't Exs. 35-38.)

II. For example: Defendant's eMule search for "linda pthc" under the "Media User" account on the Sony all-in-one desktop returned the file titled "(Pthc) Amber 7Yo (Blowjob Anal) New 2006 - 11m21S Mpg Or Linda Or Ann Holiday Old Pedo Preview.wmv." Defendant downloaded that child pornography video file on March 27, 2013 and saved the file in the eMule incoming folder. (Trial Tr. at 127-128; Gov't Ex. 35; see also Gov't Exs.

[8] "TMS Scripter" is a scripting program used for computer programming language, which allows little programs to be installed in larger programs and allows a user to write a program. (Trial Tr. 123-124.)

36-38 (connecting the three other child pornography video files to search terms Defendant used in eMule).)

JJ. Within the eMule application under the "Media User" account on the Sony all-in-one desktop, Defendant's child pornography files were available for sharing and download by other users on the eMule network through the Internet. (Gov't Ex. 70.)

KK. All child pornography video files in the "Media User" account on the Sony all-in-one desktop had "File Created/Created On" and "Last Accessed" dates ranging from March 21, 2013 to March 28, 2013.[9] (Gov't Ex. 22.)

LL. Between March 21, 2013 and March 28, 2013, Defendant viewed multiple child pornography files on the Sony all-in-one desktop and Defendant downloaded multiple child pornography files from the Internet using the eMule software on the Sony all-in-one desktop. (Gov't Ex. 33 (listing chronologically the child pornography activity on the Sony all-in-one desktop).)

MM. In addition to the child pornography files found under the "Media User" account on the Sony all-in-one desktop, Defendant also used many architecture and design programs, which

[9] A "created-on date" is the date that a file is first "created on" the volume that it resides on within a piece of computer media. (Trial Tr. at 84.) A "last accessed date" is the date it was last accessed by a user. (Id. at 293.)

were installed under the "Media User" account on the Sony all-in-one desktop. (See Gov't Exs. 47-51.)

NN. Defendant's personal files and documents were found under the "Media User" account on the Sony all-in-one desktop, including documents related to Metal Fabulous and Abco, Defendant's two companies, documents related to Defendant's church, and documents related to the "Red Sox" and "Rangers" Little League teams. (Trial Tr. at 130-133.) Examples of Defendant's personal files include:

1. Personal letter from Defendant to his son created on June 25, 2013. (Gov't Ex. 27.)
2. Falls Church Kiwanis Little League 2013 Schedule, Red Sox Line-Up, and Contact Information, listing Defendant and Defendant's wife contact information. (Gov't Ex. 29.)
3. Graphical CAD drawings of kitchen sinks listing "Metal Fabulous" as Fabricator and "Abco" as Customer. (Gov't Ex. 30.)
4. Work Order Bill from "ETO Doors" addressed to Defendant. (Gov't Ex. 31.)
5. Falls Church Ward High Priest Group Teaching Schedule, listing Defendant as the Instructor on five different dates. (Gov't Ex. 32.)

6. Description/Advertisement of "Metal Fabulous" and "Abco." (Gov't Ex. 73.)
7. Estimate from "Metal Fabulous" to customer. (Gov't Ex. 74.)
8. Picture of Defendant wearing a Red Sox T-Shirt and Baseball Cap, holding a baseball glove. (Gov't Ex. 76.)
9. Falls Church Kiwanis Little League Incident/Injury Tracking Report, prepared on March 28, 2013 and signed by Defendant. (Gov't Ex. 77.)

OO. Recently accessed Microsoft Excel spreadsheets included files with the following names:

1. "Pipe Fitting - Generic.csv"
2. "Pipe Fitting Sizes.csv"
3. "RedsoxLineup.xlsx"
4. "2013 Spring Schedule v13.xlsx"
5. "2013 Majors - Red Sox.xlsx" (Gov't Ex. 52.)

PP. Thousands of emails associated with the email accounts "Ralph@metalfabulous.com" and "RalphF@abcocorp.com" were located in the "Media User" account on the Sony all-in-one desktop. (Trial Tr. 112-113.)

QQ. Between March 21, 2013 and April 2, 2013, Defendant's activity under the "Media User" account on the Sony

all-in-one desktop included both downloading child pornography and creating personal files for his son's little league team:

1. March 21, 26, 27, and 28 of 2013: Defendant downloaded child pornography files from the Internet using the eMule software. (Trial Tr. at 129.)
2. March 25, 2013: Defendant created the Falls Church Kiwanis Little League Schedule and Red Sox Roster and Contact Information Sheet. (Gov't Ex. 29.)
3. March 28, 2013: Defendant "unzipped" recently downloaded child pornography files. (Trial. Tr. at 85, 129-130.)

RR. The Samsung hard drive (Gov't Ex. 6) contained emails dated May 5, 2009, April 13, 2010, June 1, 2010, and June 11, 2010 under the email account "ralphf@abcocorp.com" regarding the "Rangers Game Status" and were signed "Coach Freeman." (Gov't Ex. 28.)

SS. On multiple occasions, Defendant logged into his work email account, immediately searched his work email account using child pornography search terms, and then performed other searches on the Internet using the same child pornography search terms through the Google search engine. (Gov't Ex. 33.) Specifically:

1. On November 30, 2009, on the Samsung hard drive, within minutes of logging into the email address "ralphf@abcocorp.com," Defendant performed a search within this email account using the terms "pedo" and "pedo groups." After Defendant performed this initial search, Defendant then searched the Internet using the same child pornography search terms. (Trial Tr. at 145-146.)
2. On January 21, 2010, on the Samsung hard drive, after logging into the "ralphf@abcocorp.com" email account, Defendant performed a search within this email account using the term "pthc torrent." Defendant then clicked on the returned file name that included the terms "pthc" and "torrent." The file link was "broken" and did not open a file or a website. Defendant then searched the Internet using the Google search engine to search for "pthc torrent," the identical search terms used to search his work email account. (Id. at 146-147.)

TT. Over nine-thousand (9,000) child pornography still-image files were located on the Apricorn hard drive. (Trial Tr. at 86; Gov't Ex. 26.)

UU. All child pornography files on the Apricorn hard drive were created between January of 2009 and May of 2012. (Trial Tr. at 86-87; Gov't Ex. 26.)

VV. Defendant received child pornography files from the Usenet Newsgroup[10] alt.binaries.pictures.ls-series onto the Apricorn hard drive beginning in early 2009. (Trial Tr. at 136-37; Gov't Ex. 33 at 1.)

WW. On November 30, 2009, Defendant searched his work email account "RalphF@AbcoCorp.com," and subsequently the Internet, using the search terms "pedo usenet groups," similar to the Usenet Newsgroup files located on the Apricorn hard drive that were received earlier that year. (Trial Tr. at 145-46.)

XX. Between August 23, 2005 and March 29, 2013, Defendant viewed, accessed, received, and downloaded child pornography files on the computer media seized from his residence on July 30, 2013. (See Gov't Ex. 33 (listing chronologically the child pornography activity on the seized computer media).)

[10] A Usenet Newsgroup is an online common interest group that shares files and other information, typically through a user board or through email accounts. (Trial Tr. at 136-37.)

II. Elements of 18 U.S.C §§ 2252(a)(2) and (a)(4)

Recognizing that individuals distribute child pornography by gift or exchange and not solely for commercial purposes, in 1984, Congress expanded the coverage of 18 U.S.C. § 2252 to criminalize simple receipt and possession of child pornography. See H.R. Rep. 98-536, at *2 (1983), reprinted in 1984 U.S.C.C.A.N 492, 493. This amendment reflects Congress's intent to protect children from sexual exploitation and abuse. Id. at *1.

To convict Defendant of receipt of child pornography under Count One, the Government must prove the following elements beyond a reasonable doubt: (1) Defendant knowingly received a visual depiction containing child pornography; (2) the visual depiction was transported in or affecting interstate or foreign commerce, including by computer, or the visual depiction was produced using materials that had been transported in or affecting interstate or foreign commerce, including by computer; and (3) Defendant knew of the sexually explicit nature of the material and that the visual depictions were of actual minors engaged in that sexually explicit conduct. 18 U.S.C. § 2252(a)(2); see also 3-62 Modern Federal Jury Instructions-Criminal, ¶ 62.02 (Matthew Bender); United States v. Koegel, 777 F. Supp. 2d 1014, 1021 (E.D. Va. 2011).

To convict Defendant of possession of child pornography under Count Two, the Government must prove the following elements beyond a reasonable doubt: (1) Defendant knowingly possessed a visual depiction containing child pornography; (2) the visual depiction was transported in or affecting interstate or foreign commerce, including by computer, or the visual depiction was produced using materials that had been transported in or affecting interstate or foreign commerce, including by computer; and (3) Defendant knew of the sexually explicit nature of the material and that the visual depiction was of actual minors engaged in that sexually explicit conduct. 18 U.S.C. § 2252(a)(4); see also 3-62 Modern Federal Jury Instructions-Criminal, ¶ 62.02 (Matthew Bender); Koegel, 777 F. Supp. 2d at 1022.

For purposes of both Count One and Count Two, "minors" mean persons under the age of eighteen years of age. 18 U.S.C. § 2256(1). "Child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. 18 U.S.C. § 2256(8)(A). "Sexually explicit conduct" means actual or simulated (i) sexual intercourse, including genital-genital,

oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. 18 U.S.C. § 2256(2)(A); see also Koegel, 777 F. Supp. 2d at 1021.

III. Application

The Court presumes Defendant is innocent of the crimes charged in the indictment. The Court carefully considered all of the testimony and evidence admitted at trial. As the trier of fact, the Court also weighed the credibility of each witness. Based on the findings of fact discussed in detail above, the Court finds beyond a reasonable doubt Defendant knowingly received and possessed child pornography, and therefore finds Defendant guilty of both Count One and Count Two.

As an initial matter, the jurisdiction of this Court is proper because Defendant knowingly received and possessed child pornography at his residence in Falls Church, Virginia, which is within the Eastern District of Virginia. At trial, after conceding that child pornography was found on the computer media seized from Defendant's residence, the defense attempted to create reasonable doubt surrounding the open use and access to the computer media. Stated differently, the defense suggested Defendant's family members, friends of family members,

co-workers, or even strangers knowingly received and possessed the child pornography located on the computer media. The Court wholly rejects Defendant's argument. As a general matter, therefore, the Court finds the Government's evidence credible and rejects Defendant's "open access" theory as not credible and not supported by the evidence.

At trial, the Government argued that the child pornography still-image and video files contained on the Sony all-in-one desktop are the subject of the receipt charge in Count One, and the child pornography still-image and video files contained on the Apricorn hard drive are the subject of the possession charge in Count Two. (See Trial Tr. at 315; see also Gov't Trial Br. [Dkt. 54] at 1.) As discussed above, there is no question that child pornography files were contained on both the Sony all-in-one desktop and the Apricorn hard drive. (See Stipulation No. 1.) Nor is there any question that the computer media traveled in interstate commerce, satisfying the interstate nexus element. (See Stipulation No. 2.) The primary issue in determining Defendant's guilt, therefore, is whether Defendant knowingly received and possessed the child pornography, the first necessary element of each charged offense, as discussed above. The Court answers this question in the affirmative and finds Defendant guilty as charged in Count One and Count Two of the Indictment.

A. Receipt of Child Pornography under § 2252(a)(2)

To determine whether Defendant knowingly received child pornography, the Court is informed by four factors: (1) whether the child pornography files were found on Defendant's computer; (2) the number of child pornography files found; (3) whether the content of the files was evident or clear from the file names; and (4) Defendant's knowledge and ability to access the storage area of the files. United States v. Miller, 527 F.3d 54, 67 (3d Cir. 2008) (citing United States v. Irving, 452 F.3d 110, 122 (2d Cir. 2006); United States v. Payne, 341 F.3d 393, 403 (5th Cir. 2003); United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006); United States v. Kuchinski, 469 F.3d 853, 861-63 (9th Cir. 2006)). For Count One, the Court primarily considers the child pornography files located on the Sony all-in-one desktop.

1. Location of the Child Pornography Files

Thousands of child pornography still-image files and hundreds of child pornography video files were recovered from the Sony all-in-one desktop under the "Media User" account. The "Media User" account also contained a variety of architectural software and design programs, and Defendant's personal documents and files, including work orders, church teaching schedules, and little league rosters and contact information sheets. The Sony all-in-one desktop was seized from the third-floor living space

adjacent to Defendant's bedroom. Although Defendant concedes that child pornography files were on the Sony all-in-one desktop, he denies ownership or knowing receipt of the files and "maintains the government was not able to exclude the very real possibility that someone else put the images on the hard drive." Irving, 452 F.3d at 122. Just like in Irving, the Court rejects this assertion.

The defense attempted to raise a reasonable doubt as to who downloaded and possessed the child pornography files found on the Sony all-in-one desktop. First, on cross-examination, HSI Agent Varda, the computer forensic expert, testified that the computer media contained a significant amount of material not related or relevant to child pornography and reflected a variety of potential users, including Defendant's wife, mother in law, and children. (Trial Tr. at 160-186.) On the Sony all-in-one desktop under the "Media User" account, there were searches for "Dragonball Z," "Zune HD," "True Lies," and other Arnold Schwarzenegger movies, a favorite of one of Defendant's sons. (Id. at 175-176, 179.) Second, Defendant's family members testified about the "open nature" of Defendant's residence. (Id. at 195-196, 220, 272.) Defendant's oldest son, who had graduated from high school and now resides in the basement apartment of the residence, often brought unknown guests into the home, who would use the computer in the kitchen

without restriction. (Id. at 271-276.) Defendant's mother in law described some of these individuals as "troubled young men." (Id. at 220.) Defendant's wife described one son's arrest on a marijuana charge,[11] and she testified that she was informed by law enforcement that another son also might have viewed pornography.[12] (Id. at 282-283.) But these facts do not cast reasonable doubt on Defendant's knowing receipt of child pornography on the Sony all-in-one desktop. Rather, the Court finds this testimony to be a red herring, offered to eclipse Defendant's knowing receipt, albeit unsuccessfully.

The child pornography still-image files and video files were found under the Defendant's "Media User" account on

[11] Defendant's wife testified that her son was arrested on March 21, 2013, the same day that the Government's evidence shows Defendant downloaded child pornography from eMule and viewed child pornography on the Sony all-in-one desktop. The defense attempted to use the fact that Defendant later posted bond to secure his son's release from jail as an alibi defense. The Court finds this attempted alibi defense unavailing, however, because HSI Special Agent Varda testified that he could not provide an exact time Defendant downloaded or viewed the child pornography. HSI Special Agent Varda also testified regarding the "queuing process" within eMule and eDonkey, and how downloaded files can be inactive or active, dependent on various factors such as Internet connection speed and availability of other users. Thus, the Court finds Defendant downloaded and viewed child pornography earlier in the day on March 21, 2013, and proceeded to the Fairfax County Adult Detention Center later that night to post bond for his son. (See Gov't Ex. 33 at 8; see also Def. Ex. 7 (showing bond was actually posted at 1:54:31 a.m. on March 22, 2013).)

[12] Defendant's wife testified that she was notified by law enforcement that one of her sons had accessed searches on the Internet for "Lolita." (Trial Tr. at 284-286.) "Lolita" is apparently a common search term used to find child pornography. However, it is also the name of a book written by Vladimir Nabokov. And Defendant's wife adamantly denied that she had knowledge of any of her children viewing or downloading child pornography files. (Id. at 278-279.) There was no additional evidence presented to support the inference that it was Defendant's son who viewed or downloaded child pornography. Thus, the Court rejects this argument as not credible and not supported by the evidence.

his computer, the Sony all-in-one desktop. In addition to the eMule software used to download and receive child pornography, many architecture and design programs were also installed on Defendant's "Media User" account. Defendant's "Media User" account included other personal documents and files that he created for work, church, or his son's little league team. The Government's evidence established that in between downloading and receiving child pornography files using eMule from March 21, 2013 to March 28, 2013, Defendant also created his son's little league roster and contact information sheet on March 25, 2013. Defendant's downloading and receipt of child pornography was extensively intertwined with other personal word processing and work activity on the Sony all-in-one desktop and other computer media.

Moreover, the evidence at trial established that Defendant would search his work email accounts using child pornography search terms and then also search the Internet using the same terms. Thousands of emails from Defendant's email accounts were located on the computer media. Most notably, the Government's evidence established that on multiple occasions, immediately after logging into his work email accounts, Defendant would search his work email account using search terms associated with child pornography, the same search terms that were subsequently used to search the Internet or eMule for child

pornography. See United States v. Pruitt, 638 F.3d 763, 767 (11th Cir. 2011) (finding evidence that the defendant searched the Internet for child pornography on a computer containing child pornography constitutes circumstantial evidence that the defendant knowingly received child pornography). The Government additionally linked the search terms Defendant used in eMule to four child pornography video files Defendant downloaded and saved in the eMule incoming folder (See Gov't Ex. 20).

The defense correctly asserts that there is no direct evidence that places Defendant at the Sony all-in-one desktop downloading and viewing child pornography. That is not dispositive or even required, however, and while circumstantial, all of the evidence presented at trial establishes beyond a reasonable doubt that Defendant downloaded and received child pornography files under his "Media User" account on the Sony all-in-one desktop. United States v. Larman, 547 F. App'x 475, 480 (5th Cir. 2013) (holding circumstantial evidence can establish the defendant knowing received child pornography from the Internet and is sufficient to sustain a conviction for receipt of child pornography). Thus, the first factor supports the finding that Defendant knowingly received child pornography as charged in Count One.

2. Remaining Factors

The remaining factors -- number of child pornography

files found; content of the files was evident or clear from the file names; and Defendant's knowledge and ability to access the storage area of the files -- also support the finding that Defendant knowingly received child pornography. First, Defendant stored thousands of still-image files and hundreds of video files of child pornography in the eMule incoming folder. See United States v. Stanley, 533 F. App'x 325, 328 (4th Cir. 2013) (finding evidence that the defendant possessed hundreds of child pornography files located in the shared folder of the peer-to-peer program constitutes knowing receipt). Second, the content of the files was evident or clear from the file names. (See, e.g., Gov't Ex. 22 ("!!NEW!! 2010 [PTHC - Kingpass - Hussyfan] Maria 12Yo Mexican Girl giving a blowjob.mpg" or "(Pthc) 7Yo Little Linda - Trying Anal.mpg."); see also Stanley, 533 F. App'x at 328 ("The government introduced evidence of common search terms associated with child pornography, which were included in many of the file names found on the laptop.").) Third, Defendant had the knowledge and ability to access the child pornography files on the Sony all-in-one desktop, which was located steps from his bedroom. Not only did Defendant have the ability to access the files, he frequently accessed the files. (See Gov't Ex. 46 (listing frequently-accessed Window Media Player video files, all of which were child pornography video files).) Accordingly, the remaining factors also support

the finding that Defendant knowingly received child pornography.

In summation, with respect to Count One, the Government has satisfied all elements required for a conviction of receipt of child pornography under 18 U.S.C. § 2252(a)(2). The Government has proven the following elements beyond a reasonable doubt:

(1) Defendant knowingly received a visual depiction, both still images and videos, containing child pornography (see supra, III.A.1-2.);

(2) the visual depiction was transported in or affecting interstate or foreign commerce, including by computer, specifically through the Internet and downloaded via the eMule software, or the visual depiction was produced using materials that had been transported in or affecting interstate or foreign commerce, including by computer (see Stipulation No. 2 ("[The seized computer media] were manufactured outside the Commonwealth of Virginia and travelled in interstate commerce[.]")); and

(3) Defendant knew of the sexually explicit nature of the material and that the visual depictions were of actual minors engaged in that sexually explicit conduct (see supra, III.A.1-2; see also Stipulation No. 1 ("[T]he images and videos in Government Exhibits 20 and 21 depict actual children under 18-years-of-age engaged in sexually explicit conduct that

occurred outside the state of Virginia.")).

Therefore, the Court finds Defendant guilty of Count One, receipt of child pornography in violation 18 U.S.C. § 2252(a)(2).

B. Possession of Child Pornography under § 2252(a)(4)

Similarly, the Court finds that Defendant knowingly possessed child pornography on the Apricorn hard drive. The Fourth Circuit has not "formally decided whether possession is a lesser-included offense [of receipt.]" United States v. Mason, 532 F. App'x 432, 436 n.1 (4th Cir. 2013) (citing United States v. Brown, 701 F.3d 120, 125 n.6 (4th Cir. 2012)). But so long as the evidence at trial establishes that the receipt and possession charges are predicated on distinct conduct, or distinct child pornography files, separate convictions are appropriate. Mason, 532 F. App'x at 437.

Here, Defendant knowingly possessed over 9,000 still-image child pornography files contained on the Apricorn hard drive, which is distinct computer media from the Sony all-in-one desktop. (See Gov't Ex. 26.) According to the Government's evidence, Defendant created child pornography files on the Apricorn hard drive dating back to January 11, 2009 using the Usenet Newsgroup alt.binaries.pictures.ls-series. (Trial Tr. at 136-37; Gov't Ex. 33 at 1-2.) Later, on November 30, 2009, Defendant searched his work email account and the Internet using

search terms "pedo usenet newgroup," which is almost identical to the Usenet Newsgroup Defendant used to facilitate his possession of child pornography on the Apricorn hard drive. (Trial. Tr. at 145-46.) Moreover, beginning in 2011 and continuing into 2012, Defendant's possession of child pornography activity alternated between the Sony all-in-one desktop, the Apricorn hard drive, and other computer media. (Gov't Ex. 33 at 4-7.) During this period of time, Defendant regularly accessed and viewed child pornography files that he possessed on the Apricorn hard drive. (Id.) This circumstantial evidence proves beyond a reasonable doubt that Defendant knowingly possessed the child pornography files on the Apricorn hard drive.

Accordingly, the Government has satisfied all elements required for a conviction of possession of child pornography under 18 U.S.C. § 2252(a)(4). The Government has proven beyond the following elements beyond a reasonable doubt: (1) Defendant knowingly possessed over 9,000 still-image files of child pornography on the Apricorn hard drive (see supra, III.B.); (2) those still-image files were transported in or affecting interstate, including by computer, or were produced using materials that had been transported in or affecting interstate or foreign commerce, including by computer (see Stipulation No. 2); and (3) Defendant knew of the sexually explicit nature of

still-image files on the Apricorn hard drive and that the visual depictions were of actual minors engaged in that sexually explicit conduct (see Gov't Ex. 26).

Therefore, the Court finds Defendant guilty of Count Two, possession of child pornography in violation of 18 U.S.C. § 2252(a)(4).

IV. Conclusion

For the foregoing reasons discussed above, the Court makes the following findings of fact and conclusions of law:

(1) The Court has jurisdiction over this matter because Defendant knowingly received and possessed child pornography at his residence in Falls Church, Virginia, which is within the Eastern District of Virginia;

(2) The Court finds Defendant guilty of one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) (Count One); and

(3) The Court finds Defendant guilty of one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4) (Count Two).

An appropriate Order shall issue.

/s/
James C. Cacheris
UNITED STATES DISTRICT COURT JUDGE

January 2, 2015
Alexandria, Virginia